DETECTIFY CASE STUDY: VISMA

How Visma effectively prevents subdomain takeovers and receives less false positives

AN INTERVIEW WITH:

Catalin Curelaru

SECURITY TRIAGE LEAD

VISMA

detectify

Visma's set up & security challenges

A remote work setting and many employees at Visma keep their security team busy. **Catalin Curelaru, Security Triage Lead at Visma**, specializes in infrastructure and product security areas with strong knowledge of security operations.

"We have over 5000 developers, 40 acquisitions per year, over 150 companies at Visma, and employees spread across 37 countries" says Catalin.

Visma's security challenges

- Subdomain takeovers
- Exposed tokens
- Legacy system
- OWASP top 10 vulnerabilites coverage
- False positives

About Visma

Visma is a privately held software company that simplifies core business processes in the private and public sectors.

Industry:	Software
Company size:	Enterprise (12,000 employees)
Location:	Headquartered in Oslo, with over 200 local offices

Catalin Curelaru

SECURITY TRIAGE LEAD

How Visma benefits from built-in ethical hacker research

"We used other tools before, but we chose Detectify because it helps us reduce false positives and gets much information from the availability perspective," explains Catalin.

The ethical hacker knowledge from Crowdsource adds extra value to Visma's security journey. Visma views using Detectify as complementary to a bug bounty program and internal penetration testing teams as an extra security layer.

"We are a big team with a vast amount of public products that need to be assessed. However, with the limited amount of penetration testers in the teams, we cannot cover all the applications from all the security angles. That's why you need Detectify Crowdsource," explains Catalin.

> *“We chose Detectify because it helps us reduce false positives and gets much information from the availability perspective"*

Detectify Crowdsource

Crowdsource uses the power of elite ethical hackers to submit new and undocumented vulnerabilities. Its unique bounty model means ethical hackers are paid based on hits on a vulnerability type rather than a one-off payment.

These vulnerability findings become security tests built daily into Detectify's products, Application Scan and Surface Monitoring. As a result, you can scan your systems for the newest vulnerabilities before everyone else.

How Visma uses Detectify

Visma has been using Detectify for several years now, resulting in a strong working partnership and trends over time. When using Application Scanning and Surface Monitoring, they have seen that Detectify consistently delivers vulnerabilities with a very low false-positive rate. They know they can trust the data coming from the reports and act quickly upon it.

To address and reduce subdomain takeovers, Visma's teams use Asset Monitoring. "We have multiple public applications, and we want to be 100% sure that we are free from subdomain takeovers. Detectify helps us achieve that," says Catalin.

Scanning frequency

Visma runs weekly Application Scans combined with Surface Monitoring. The Application Scan scanning frequency depends on each team and their scheduled time preferences.

Dealing with critical vulnerabilities

Visma's security team doesn't have direct access to all servers and environments as each team is responsible for their infrastructure and remediations. With Detectify's Slack integration, Visma gets high severity vulnerability finding alerts instantly across their applications as soon as they are discovered. All other issues are triaged in Jira. "It's our responsibility as a company to be 100% sure that we address critical security issues on time," says Catalin.

> *"We have multiple public applications, and we want to be 100% sure that we are free from subdomain takeovers. Detectify helps us achieve that"*

Results

Securing M&A process

Detectify takes an essential part of the DAST process during the M&As at Visma, ensuring the desired security posture. Detectify helps newly acquired companies discover previously unknown security issues. “This is the main ROI when certain development teams get valuable information and can strengthen their security,” says Catalin.

Less noise, more relevant findings

Catalin explained that the central realization they had while using Detectify was a decrease in vulnerability findings. He explained that sometimes their teams were concerned about not receiving many results. This meant they received more relevant findings and less noise which ensured teams were doing a great job.

For the full version of the case study visit:

www.detectify.com/case-studies/visma

Catalin’s security tips

- To use OWASP SAMM bottom up approach
- Rely on OWASP best practices
- Use multiple tools - SAST, DAST, third party scanning, Red Team/Purple Teaming

go hack
yourself.